Remarks

This is in response to the final Office Action mailed on February 24, 2006. Claims 1-33 and 35-37 remain pending. Reconsideration and allowance are requested for the following reasons.

I. Interview Summary

Applicants appreciate the courtesy extended by the Examiner to Applicants' representative, Robert A. Kalinsky, during the telephonic interview on May 3, 2006. During the interview, claims 1, 31, and 33 and U.S. Patent Nos. 5,983,207 and 5,999,622 were discuss ed. No agreement regarding the allowability of the claims was reached.

II. Claims 1-32

In section 3 of the Action, claims 1-32 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Turk et al., U.S. Patent No. 5,983,207, in view of Yasuk awa et al., U.S. Patent No. 5,999,622. This rejection is respectfully traversed.

Claim 1 recites means for decoding the encoded data item to retrieve the data item from the separately stored parts, whereby the data item is retrievable even if some of the parts are lost or corrupted.

To establish a prima facie case of obviousness, the references, when combined, must teach or suggest all the claim limitations. See In re Vaeck, 20 USPQ2d 1438 (Fed. Cir. 1991); MPEP 2143 et seq.

For at least the following reasons, neither Turk nor Yasukawa, alone or in combination, discloses or suggests all of the limitations, namely that a data item is retrievable even if some of the parts are lost or corrupted, as recited by claim 1. It is therefore suggested that the combination of Turk and Yasukawa fails to render the rejected claims unpatentable.

The Office Action fails to identify any disclosure suggesting that a data item is retrievable even if some of the parts are lost or corrupted. For example, the Action identifies the "private key" of the public key encryption technology disclosed by Turk as being used to decrypt electronic data. However, Turk fails to disclose or suggest that a private key can be used to decrypt electronic data if some of the parts of the electronic data are lost or corrupted. In fact, a private key is defined simply as follows: "One of two keys in public key encryption. The user

keeps the private key secret and uses it to encrypt digital signatures and to decrypt received messages." Microsoft Computer Dictionary, Fourth Edition, p. 358 (1999). As this definition illustrates, Turk's disclosure regarding the use of a private key does not suggest that electronic data including parts that are lost or corrupted can be decrypted using the private key.

Yasukawa discloses an encryption scheme wherein individual segments of a file are selectively encrypted. Yasukawa, col. 3, ll. 43-52. However, Yasukawa once again fails to disclose or suggest that the file can be decrypted if some of the parts of the file are lost or corrupted.

Reconsideration and allowance of claim 1, as well as claims 2-30 and 36 that depend therefrom, are therefore requested for at least these reasons.

Claim 31 is directed at a method of storing digital data items, including decoding a data item to retrieve the data item from the separately stored parts, whereby the data item is retrievable even if some of the parts are lost or corrupted. Claim 31, as well as claim 32 that depends therefrom, is therefore allowable for at least similar reasons to those provided above with respect to claim 1. Reconsideration and allowance are requested.

III. Claim 36

In section 4 of the Action, claim 36 stands rejected under 35 U.S.C. § 103(a) as being unpatentable over Turk in view of Yasukawa and further in view of Chiu, U.S. Patent No. 6,181,336. This rejection is respectfully traversed.

Chiu does not remedy the shortcomings of Turk and Yasukawa noted above. Claim 36 depends from claim 1 and is allowable for at least the same reasons as those noted above with respect to claim 1. Reconsideration and allowance are requested.

IV. Claims 33 and 35

In section 5 of the Action, claims 33 and 35 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Carroll, U.S. Patent No. 6,105,131, in view of Yasukawa. This rejection is respectfully traversed.

Claim 33 recites decoding an encoded item to retrieve the item from separately stored parts, whereby the item is retrievable even if some of the parts are lost or corrupted. Neither Carroll nor Yasukawa discloses or suggests such a limitation.

For example, while Carroll discloses use of encryption, digital signatures, and digital certificates to secure the system from unauthorized access (see col. 1, l. 58 - col. 2, l. 8; col. 5, ll. 53-55; and col. 6, ll. 6-11), Carroll fails to disclose or suggest that such techniques can be used to decode an item even if some of the parts are lost or corrupted.

Reconsideration and allowance of claim 33, as well as claim 35 that depends therefrom, are requested.

V. Claim 37

In section 6 of the Action, claim 37 stands rejected under 35 U.S.C. § 103(a) as being unpatentable over Carroll in view of Yasukawa and further in view of Chiu. This rejection is respectfully traversed.

Chiu does not remedy the shortcomings of Turk, Carroll, and Yasukawa noted above. Claim 37 depends from claim 31 and is allowable for at least the same reasons as those noted above with respect to claim 31. Reconsideration and allowance are requested.

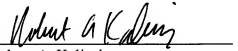
VI. Conclusion

The remarks set forth above provide certain arguments in support of the patentability of the pending claims. There may be other reasons that the pending claims are patentably distinct over the cited references, and the right to raise any such other reasons or arguments in the future is expressly reserved.

Favorable reconsideration in the form of a Notice of Allowance is requested. Please contact the undersigned attorney with any questions regarding this application.

Respectfully submitted,
MERCHANT & GOULD P.C.
P.O. Box 2903
Minneapolis, Minnesota 55402-0903
(612) 332-5300

Date: June 22, 2006



Robert A. Kalinsky
Reg. No.: 50,471